SOLUTION OVERVIEW

BIG-IP DNS for Service Providers

A carrier-grade DNS-resolving solution with hyperscaling and security services that enables fast, low-latency web browsing.

KEY FEATURES

Reduced network latency
IP Anycast integration distributes the DNS request load and directs single IP requests to multiple local devices

Lower LDNS latency
Enables caching and resolving by offloading LDNS and backend DNS infrastructure

DNS over HTTPS (DoH)
Resolve DNS queries from DoH-enabled web browser queries to mitigate SSL as an attack vector and retain control over traffic on network

Attack mitigation
Shields DNS from reflection or amplification DDoS attacks with BIG-IP AFM™, an ICSA network firewall certified platform

Authoritative DNS
Hyperscales responses up to 100 million RPS with DNS Express enabled in Rapid Response Mode (RRM)

DNS inline services
Manages network traffic with high availability to DNS and caching ENUM services

3G, 4G, and 5G 3GPP support
Supports NAPTR DNS nodes and services to drive faster service instantiation

Logging, reporting, and analytics
Detailed DNS and GSLB data, statistics, and graphs for in-depth analysis

Service availability for best performance
Geographic load balancing identifies location at the continent, country, or state level and connects users to the closest app

Scaling DNS Service with BIG-IP DNS

With network traffic growing dramatically to support new mobile users and applications, service providers need a scalable, secure DNS solution that enables faster web browsing and low latency. F5® BIG-IP® DNS provides an intelligent way to respond to DNS queries by enabling an optimized local DNS (LDNS) infrastructure and a better-quality user experience to increase revenue and reduce subscriber churn.

SCALING, SECURING, AND OPTIMIZING DNS

DNS, a core Internet technology, enables subscribers to access services, making it one of the most important components in the network infrastructure. If DNS is unavailable, subscriber services will not function properly.

Service providers need to build an optimized and secure DNS infrastructure to better serve their subscribers today and in the future. Creating this infrastructure requires a tremendous amount of real-time management, stability, and room to grow. The ability to rapidly scale DNS becomes a critical issue when dealing with millions of service names and IP addresses. As a provider scales the control plane and looks to automate the mobile core, he also needs to ensure the security of subscriber and billing data, as well as the capacity to withstand attacks. The first step to protect the network from attacks is to understand the DNS environment and actively monitor DNS traffic, not only for uptime but for load and resource usage in real time.

While an efficient and secure DNS infrastructure remains a vital part of a service provider's offering, it presents serious implementation and management challenges. BIG-IP DNS addresses these with hyperscaling and security services.

F5 BIG-IP DNS—A SCALABLE DNS SOLUTION

The F5 BIG-IP DNS solution helps service providers optimize and secure their DNS infrastructures and traffic flows with a carrier-grade, secure, high-performance, and authoritative DNS-resolving solution that also includes caching and resolving capabilities. BIG-IP DNS delivers an intelligent and scalable DNS infrastructure that gives mobile users faster access to services. BIG-IP DNS load balances local and recursive DNS services and enables a DNS64 environment, creating a fault-tolerant architecture that optimizes network traffic and improves user experiences.

To support subscriber growth while reducing DNS server count, BIG-IP DNS hyperscales DNS services and responds authoritatively to DNS queries up to 100 million query responses per second (RPS). The caching and resolving functions in BIG-IP DNS offload LDNS infrastructure and backend DNS services with a much faster response to subscriber queries while dramatically reducing latency. These efficiencies increase average revenue per unit (ARPU), improving monetization of services.

KEY FEATURES (CONT.)

IPv6 and DNS64 support
Translates traffic for consumption by either IPv4 or IPv6 endpoints

Real-time DNSSEC
Protects LDNS servers from cache poisoning and man-in-the-middle attacks

KEY BENEFITS

The BIG-IP platform provides the following DNS services:

- Authoritative DNS hyperscalability, handling millions of global name requests per second
- Consolidation and offloading of LDNS with high-performance DNS caching and resolving
- DNS delivery performance for both inline and recursive DNS
- DNS DDoS mitigation, query validation, traffic inspection and manipulation, and malicious IP blocking
- Consolidation at the heart of the network of firewall, load balancing, URL filtering, policy enforcement, NAT64 and DNS64 translation and F5 iRules that reduce CapEx and OpEx by enabling a significant reduction in the number of servers
- Automation of packet gateway selection using DNS and global server load-balancing services for optimized service experiences
- Translates traffic for consumption by either IPv4 or IPv6 endpoints
- Resolve DNS queries from DoH-enabled web browser queries to mitigate SSL as an attack vector and retain control over traffic on the network

BIG-IP DNS works with other F5 service delivery solutions for NAT64 translation, subscriber and application awareness with policy enforcement, and high-performance service delivery. This integration creates a complete service delivery infrastructure that optimizes and secures DNS infrastructure while boosting subscriber satisfaction.

DNS over HTTPS (DoH)

DoH is fully enabled by popular web browsers and can create security issues for service providers who are not able to terminate and respond to these DNS inquires. F5 BIG-IP DNS allows service providers to terminate and resolve DNS queries over HTTPS without impacting responses-per-second (RPS). DoH support removes HTTPS as an attack vector for malicious domains.

3G, 4G and 5G (3GPP) weighted resolution

BIG-IP DNS supports name authority pointer (NAPTR) with service records (SRV) to help drive fast resolution of DNS queries for 3G, 4G and 5G services. BIG-IP's 5G 3GPP support adheres to 3GPP TS 29.303 R16 specification for weighted DNS query resolution. Multi-band mobility service support enables consolidated and simplified DNS resolution infrastructure.

COMPREHENSIVE DNS SECURITY

DNSSEC

BIG-IP DNS enables IT administrators to set up DNS security extensions (DNSSEC) to validate signing keys and ensure connected DNS servers are the right ones. This eliminates masquerading and spoofing of Authoritative DNS services and creates a trusted DNS chain for resolved DNS queries.

DNS distributed denial of service (DDoS) attacks

BIG-IP DNS includes a comprehensive security solution to protect your DNS infrastructure from common DNS DDoS attacks by hyperscaling up to 100 million query RPS in rapid response mode (RRM) for attack mitigation. Combined with BIG-IP AFM, BIG-IP DNS shields DNS from volumetric attacks—such as UDP floods, reflection, or amplification DDoS attacks—while providing the ability to inspect, validate and control DNS through protocol validation and rate-limiting for NXDOMAIN floods and malformed packets. Service providers can mitigate DNS threats by blocking access to malicious IP domains with outbound domain filtering using BIG-IP DNS response policy zones.

BIG-IP DNS helps you understand attacks with monitoring, alerting, logging, and analytics. These tools give you a global view of your infrastructure with the means to manage the network and add polices to ensure the highest availability for your business-critical applications.

The need for real-time visibility into DNS DDoS is critical. F5 BIG-IQ® Centralized Management can be used to measure device health and investigate DDoS attacks. DNS DDoS attack details can be observed by all managed F5 BIG-IP products, providing a high-level, at-a-glance view of DNS and DDoS traffic details from which you can review current traffic trends or drill down into a specific attack with criteria like attack type, size, flow history, source and destination IP address, and others.

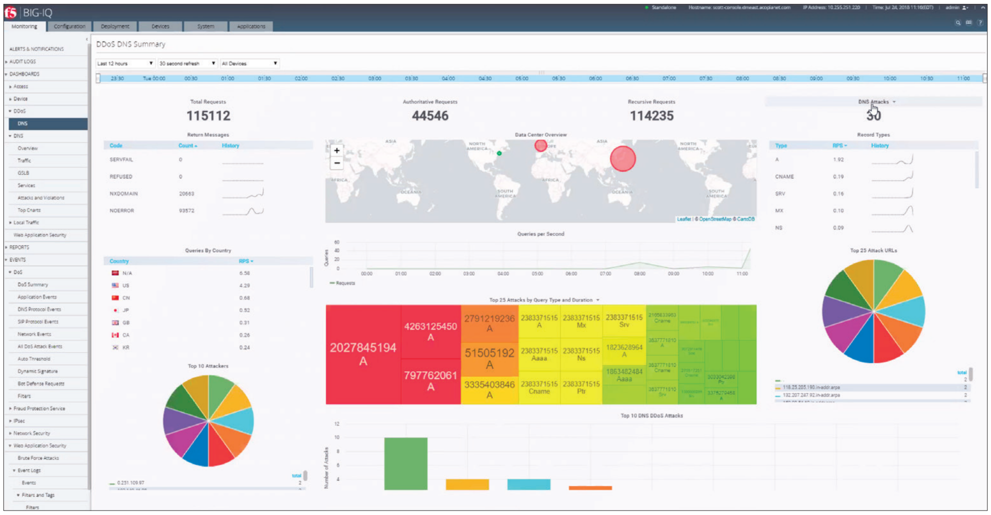

Figure 1: DNS DDoS attack details can be observed by all BIG-IQ managed BIG-IP products

As shown in Figure 1, the DNS DDoS summary page allows you to see DNS activity analytics and DDoS metrics. This gives both SOC and DNS NOC engineers the tools to accurately determine what is happening in their DNS infrastructure at a glance with the option to drill down for more detail. A Data Center Activity Map displays load at each location. The bigger or redder the circle, the more activity each location is experiencing. A queries-per-second line graph gives you a high-level view of DNS queries across all BIG-IP systems in your environment. The attack heat map provides an extremely quick view of the top attacks on the infrastructure, sorted and color-coded by size and severity. If your customers' network experiences tens of thousands of DNS attacks a day, this is the most efficient way to zero in on the attacks that matter most.

THE NEED FOR REAL-TIME VISIBILITY INTO DNS DDOS IS CRITICAL. F5 BIG-IQ® CENTRALIZED MANAGEMENT CAN BE USED TO MEASURE DEVICE HEALTH AND INVESTIGATE DDOS ATTACKS.

Hardware or virtual deployment options

The BIG-IP DNS solution is available as a physical or a virtual solution. BIG-IP DNS with F5® DNS Express® enabled in rapid response mode (RRM) in a fully loaded chassis hyperscales up to 100 million RPS. Each Virtual Edition (VE) can provide 250k RPS. The DNS NFV packaged solution is available in 500k and 2m query response per second (QPS) increments and the DNS security NFV packaged solution is available in 250k, 500k and 2m QPS increments. NFV packaged solutions include the VNF Manager for self-configuration and lifecycle management. All solutions are available to purchase with a perpetual license or a subscription license.

Conclusion

DNS solutions are critical to consumer quality of experience when browsing the internet. F5 solutions enable faster web browsing and lower latency for subscribers, which provides improved subscriber satisfaction. For service providers, higher ARPU and lower subscriber churn results from an architecture designed for maximum efficiency and monetization—handling millions of subscribers from multiple network device types.

F5 DNS solutions provide unrivalled network and subscriber security that mitigates DNS threats and in-network attacks, blocks access to malicious IPs, and provides the ability to monitor, alert, log, inspect, and validate DNS content.

ARCHITECTURE DESIGNED FOR MAXIMUM EFFICIENCY AND MONETIZATION—HANDLING MILLIONS OF SUBSCRIBERS FROM MULTIPLE NETWORK DEVICE TYPES.

More Information

Learn more about F5 BIG-IP DNS Solutions

Near real-time DNS reporting mitigates DDoS attacks
Gain insight into Load-Aware Entity Location with BIG-IP DNS Services